A UNIVERSAL SIGNATURE OBJECT FOR DIGITAL DATA

Inventors:

Eng Whatt Toh

Kok Khuan Fong

Raj Maharjan Madhav

Kok Hoon Teo

RELATED APPLICATIONS

[0001] This application claims priority under 35 U.S.C. § 119(e) to commonly-assigned U.S. Provisional Patent Application Serial No. 60/242,113, "Universal Object For E-Signed Digital Contents," by Eng-Whatt Toh, filed 19 October 2000; and commonly-assigned U.S. Provisional Patent Application Serial No. 60/242,013, "Efficient Method For Routing Deliveries Through Recipient Translation," by Eng-Whatt Toh, filed 19 October 2000. The subject matters of the foregoing applications are incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] The present invention relates generally to digital signatures. More particularly, the invention relates to computer-implemented systems and techniques for binding a digital signature to digital data regardless of the file format of the digital data, and for utilizing the same.

2. Description of Background Art

[0003] With the increased use of computers, a great many items both in business and in people's personal lives exist, at some point, in digital form. These items include business documents, digital audio, digital video, pamphlets, presentations, digital graphics, and even computer applications and programs. Technology now exists to transact and trade entirely in digital form. Since items can readily be exchanged digitally, the need for physical copies has been lessened. Furthermore, law-making entities of different countries have legitimized digital signatures as being equivalent to traditional, or wet, signatures. With these laws, it is now possible for people and businesses to transact by exchanging electronic documents and applying their digital signatures without ever using hard copies.

[0004] Electronic signature technologies are based on cryptography. Cryptographic algorithms can generally be divided into two classes: symmetric key cryptography and asymmetric key cryptography. Of the two types, asymmetric key cryptography is used to generate digital signatures.

[0005] Asymmetric key encryption, also called public-key encryption, involves a pair of keys — a public key and a private key. The keys themselves are typically large numbers derived from complex mathematical algorithms. These keys are used to encrypt and/or decrypt digital data. Once a user has a key pair, the user typically keeps the private key secret but publishes the corresponding public key. The public key and the private key are mathematically related so that one key can decrypt data encrypted by the other key. However, the mathematical relationship between the keys is sufficiently complex that it is computationally infeasible to derive one key given the other.

[0006] One application of public-key encryption is secure data delivery. Thus, if a sender wants to send data to a recipient in a manner such that only the recipient can read the data, the sender can encrypt the data with the recipient's public key. Since only the recipient's private key

can decrypt the data, the sender can be assured that only the recipient can read the data, assuming that the recipient is the only one with access to the private key.

[0007] In addition to encrypting data so that only specific individuals can decrypt the data, public-key encryption can also be used for digital signatures. For example, public-key encryption allows the recipient of digitally signed data to verify the identity of the signatory. Assuming that the data is encrypted using the signatory's private key, it can be decrypted only by the corresponding public key. If a recipient can decrypt data using the signatory's public key, he can be assured that the data was originally encrypted using the corresponding private key. Thus, the recipient can be assured that the signatory was the one who encrypted the data. In other words, the signatory has digitally signed the data.

[0008] However, for this identification to be effective, the recipient must receive the signatory's public key in a manner in which the recipient trusts that the key is in fact the signatory's public key and not someone else's public key. This trusted transmission of the signatory's public key can occur in several ways. For example, the signatory could personally give the public key to the recipient. Alternatively, the signatory could deliver the public key via a trusted delivery service.

[0009] Another possible method is to link the signatory to his public key by a digital certificate issued by a trusted third party. A digital certificate is a digital document that identifies a certain public key as belonging to, or is associated with, a certain entity, such as an individual, a legal entity, a Web server, or the like, in a trustworthy manner. A trusted third party, known as a certificate authority ("CA"), typically issues a digital certificate. The CA issues a certificate that identifies, among other things, an entity and that entity's public key. In this manner, the CA acts like a notary, attesting that a certain key belongs to a certain entity. A recipient who trusts the CA can be assured that any data decrypted with that public key must have been encrypted with the corresponding private key, and if only the signatory has access to that private key, the recipient knows that the signatory encrypted the data.